(ix) Review, if applicable, ongoing Computer Matching Agreements. The Defense Data Integrity Board approves Computer Matching Agreements for 18 months, with an option to renew for an additional year. This additional review will ensure that the requirements of the Privacy Act, Office of Management and Budget guidance, local regulations, and the requirements contained in the Matching Agreements themselves have been met.

(7) All DA personnel will—

(i) Take appropriate actions to ensure personal information contained in a Privacy Act system of records is protected so that the security and confidentiality of the information is preserved;

(ii) Not disclose any personal information contained in a Privacy Act system of records except as authorized by 5 U.S.C. 552a, DOD 5400.11–R, or other applicable laws. Personnel willfully making a prohibited disclosure are subject to possible criminal penalties and/or administrative sanctions; and

(iii) Report any unauthorized disclosures or unauthorized maintenance of new Privacy Act systems of records to the applicable activity's Privacy Act Official.

(8) Heads of Joint Service agencies or commands for which the Army is the Executive Agent or the Army otherwise provides fiscal, logistical, or administrative support, will adhere to the policies and procedures in this part.

(9) Commander, Army and Air Force Exchange Service, will supervise and execute the Privacy Program within that command pursuant to this part.

(10) Overall Government-wide responsibility for implementation of the Privacy Act is the Office of Management and Budget. The Department of Defense is responsible for implementation of the Act within the armed services. The Privacy Act also assigns specific Government-wide responsibilities to the Office of Personnel Management and the General Services Administration.

(11) Government-wide Privacy Act systems of records notices are available at *http://www.defenselink.mil/privacy*.

(e) *Legal Authority*. (1) Title 5, United States Code, Section 552a, as amended, The Privacy Act of 1974.

(2) Title 5, United States Code, Section 552, The Freedom of Information Act (FOIA).

(3) Office of Personnel Management, Federal Personnel Manual (5 CFR parts 293, 294, 297, and 7351).

(4) OMB Circular No. A–130, Management of Federal Information Resources, Revised, August 2003.

(5) DOD Directive 5400.11, Department of Defense Privacy Program, November 16, 2004.

(6) DOD Regulation 5400.11–R, Department of Defense Privacy Program, August 1983.

(7) Title 10, United States Code, Section 3013, Secretary of the Army.

(8) Executive Order No. 9397, Numbering System for Federal Accounts Relating to Individual Persons, November 30, 1943.

(9) Public Law 100–503, the Computer Matching and Privacy Act of 1974.

(10) Public Law 107–347, Section 208, Electronic Government (E-Gov) Act of 2002.

(11) DOD Regulation 6025.18–R, DOD Health Information Privacy Regulation, January 24, 2003.

§ 505.2 General provisions.

(a) *Individual privacy rights policy*. Army policy concerning the privacy rights of individuals and the Army's responsibilities for compliance with the Privacy Act are as follows—

(1) Protect the privacy of United States living citizens and aliens lawfully admitted for permanent residence from unwarranted intrusion.

(2) Deceased individuals do not have Privacy Act rights, nor do executors or next-of-kin in general. However, immediate family members may have limited privacy rights in the manner of death details and funeral arrangements of the deceased individual. Family members often use the deceased individual's Social Security Number (SSN) for federal entitlements; appropriate safeguards must be implemented to protect the deceased individual's SSN from release. Also, the Health Insurance Portability and Accountability

Act extends protection to certain medical information contained in a deceased individual's medical records.

(3) Personally identifiable health information of individuals, both living and deceased, shall not be used or disclosed except for specifically permitted purposes.

(4) Maintain only such information about an individual that is necessary to accomplish the Army's mission.

(5) Maintain only personal information that is timely, accurate, complete, and relevant to the collection purpose.

(6) Safeguard personal information to prevent unauthorized use, access, disclosure, alteration, or destruction.

(7) Maintain records for the minimum time required in accordance with an approved National Archives and Records Administration record disposition.

(8) Let individuals know what Privacy Act records the Army maintains by publishing Privacy Act system of records notices in the FEDERAL REGISTER. This will enable individuals to review and make copies of these records, subject to the exemptions authorized by law and approved by the Secretary of the Army. Department of the Army Privacy Act systems of records notices are available at *http://www.defenselink.mil/privacy*.

(9) Permit individuals to correct and amend records about themselves which they can prove are factually in error, not timely, not complete, not accurate, or not relevant.

(10) Allow individuals to request an administrative review of decisions that deny them access to or the right to amend their records.

(11) Act on all requests promptly, accurately, and fairly.

(12) Keep paper and electronic records that are retrieved by name or personal identifier only in approved Privacy Act systems of records.

(13) Maintain no records describing how an individual exercises his or her rights guaranteed by the First Amendment (freedom of religion, freedom of political beliefs, freedom of speech and press, freedom of peaceful assemblage, and petition) unless expressly authorized by statute, pertinent to and within the scope of an authorized law enforcement activity, or otherwise authorized by law or regulation.

(14) Maintain appropriate administrative technical and physical safeguards to ensure records are protected from unauthorized alteration or disclosure.

(b) *Safeguard personal information.* (1) Privacy Act data will be afforded reasonable safeguards to prevent inadvertent or unauthorized disclosure of records during processing, storage, transmission, and disposal.

(2) Personal information should never be placed on shared drives that are accessed by groups of individuals unless each person has an ''official need to know'' the information in the performance of official duties.

(3) Safeguarding methods must strike a balance between the sensitivity of the data, need for accuracy and reliability for operations, general security of the area, and cost of the safeguards. In some situations, a password may be enough protection for an automated system with a log-on protocol. For additional guidance on safeguarding personal information in automated records see AR 380–67, The Department of the Army Personnel Security Program.

(c) *Conveying privacy protected data electronically via e-mail and the World Wide Web.* (1) Unencrypted electronic transmission of privacy protected data makes the Army vulnerable to information interception which can cause serious harm to the individual and the accomplishment of the Army's mission.

(2) The Privacy Act requires that appropriate technical safeguards be established, based on the media (e.g., paper, electronic) involved, to ensure the security of the records and to prevent compromise or misuse during transfer.

(3) Privacy Web sites and hosted systems with privacy-protected data will employ secure sockets layers (SSL) and Public Key Infrastructure (PKI) encryption certificates or other DoD-approved commercially available certificates for server authentication and client/server authentication. Individuals who transmit data containing personally identifiable information over e-mail will employ PKI or other DoD-approved certificates.

(4) When sending Privacy Act protected information within the Army using encrypted or dedicated lines, ensure that—

(i) There is an ''official need to know'' for each addressee (including ''cc'' addressees); and

(ii) The Privacy Act protected information is marked For Official Use Only (FOUO) to inform the recipient of limitations on further dissemination. For example, add FOUO to the beginning of an e-mail message, along with the following language: ''This contains FOR OFFICIAL USE ONLY (FOUO) information which is protected under the Privacy Act of 1974 and AR 340–21, The Army Privacy Program. Do not further disseminate this information without the permission of the sender.''

(iii) Do not indiscriminately apply this statement. Use it only in situations when actually transmitting protected Privacy Act information.

(iv) For additional information about marking documents ''FOUO'' review AR 25–55, Chapter IV.

(5) Add appropriate ''Privacy and Security Notices'' at major Web site entry points. Refer to AR 25–1, para 6–4n for requirements for posting ''Privacy and Security Notices'' on public Web sites. Procedures related to the establishing, operating, and maintaining of unclassified DA Web sites can be accessed at *http://www.defenselink.mil/webmasters/policy/DOD_web_policy*.

(6) Ensure public Web sites comply with policies regarding restrictions on persistent and third party cookies. The Army prohibits both persistent and third part cookies. (see AR 25–1, para 6–4n)

(7) A Privacy Advisory is required on Web sites which host information systems soliciting personally identifying information, even when not maintained in a Privacy Act system of records. The Privacy Advisory informs the individual why the information is solicited and how it will be used. Post the Privacy Advisory to the Web site page where the information is being solicited, or to a well marked hyperlink stating ''Privacy Advisory—Please refer to the Privacy and Security Notice that describes why this information is collected and how it will be used.''

(d) *Protecting records containing personal identifiers such as names and Social Security Numbers.* (1) Only those records covered by a Privacy Act system of records notice may be arranged to permit retrieval by a personal identifier (e.g., an individual's name or Social Security Number). AR 25–400–2, paragraph 6–2 requires all records covered by a Privacy Act system of records notice to include the system of record identification number on the record label to serve as a reminder that the information contained within must be safeguarded.

(2) Use a coversheet or DA Label 87 (For Official Use Only) for individual records not contained in properly labeled file folders or cabinets.

(3) When developing a coversheet, the following is an example of a statement that you may use: ''The information contained within is FOR OFFICIAL USE ONLY (FOUO) and protected by the Privacy Act of 1974.''

(e) *Notification of Individuals when personal information is lost, stolen, or compromised.* (1) Whenever an Army organization becomes aware the protected personal information pertaining to a Service member, civilian employee (appropriated or non-appropriated fund), military retiree, family member, or another individual affiliated with Army organization (e.g., volunteer) has been lost, stolen, or compromised, the organization shall inform the affected individuals as soon as possible, but not later than ten days after the loss or compromise of protected personal information is discovered.

(2) At a minimum, the organization shall advise individuals of what specific data was involved; the circumstances surrounding the loss, theft, or compromise; and what protective actions the individual can take.

(3) If Army organizations are unable to comply with policy, they will immediately notify their superiors, who will submit a memorandum through the chain of command to the Administrative Assistant of the Secretary of the Army to explain why the affected individuals or population's personal information has been lost, stolen, or compromised.

(4) This policy is also applicable to Army contractors who collect, maintain, use, or disseminate protected personal information on behalf of the organization.

(f) *Federal government contractors' compliance.* (1) When a DA activity contracts for the design, development, or operation of a Privacy Act system of records in order to accomplish a DA mission, the agency must apply the requirements of the Privacy Act to the contractor and its employees working on the contract (See 48 CFR part 24 and other applicable supplements to the FAR; 32 CFR part 310).

(2) System Managers will review annually, contracts contained within the system(s) of records under their responsibility, to determine which ones contain provisions relating to the design, development, or operation of a Privacy Act system of records.

(3) Contractors are considered employees of the Army for the purpose of the sanction provisions of the Privacy Act during the performance of the contract requirements.

(4) Disclosing records to a contractor for use in performing the requirements of an authorized DA contract is considered a disclosure within the agency under exception (b)(1), ''Official Need to Know'', of the Act.

§ 505.3 Privacy Act systems of records.

(a) *Systems of records.* (1) A system of records is a group of records under the control of a DA activity that are retrieved by an individual's name or by some identifying number, symbol, or other identifying particular assigned to an individual.

(2) Privacy Act systems of records must be—

(i) Authorized by Federal statute or an Executive Order;

(ii) Needed to carry out DA's mission; and

(iii) Published in the FEDERAL REGISTER in a system of records notice, which will provide the public an opportunity to comment before DA implements or changes the system.

(3) The mere fact that records are retrievable by a name or personal identifier is not enough. Records must actually be retrieved by a name or personal identifier. Records in a group of records that may be retrieved by a name or personal identifier but are not normally retrieved by this method are not covered by this part. However, they are covered by AR 25–55, the Department of the Army Freedom of Information Act Program.

(4) The existence of a statute or Executive Order mandating the maintenance of a system of records to perform an authorized activity does not abolish the responsibility to ensure the information in the system of records is relevant and necessary to perform the authorized activity.

(b) *Privacy Act system of records notices.* (1) DA must publish notices in the FEDERAL REGISTER on new, amended, altered, or deleted systems of records to inform the public of the Privacy Act systems of records that it maintains. The Privacy Act requires submission of new or significantly changed systems of records to OMB and both houses of Congress before publication in the FEDERAL REGISTER (See Appendix E of this part).

(2) Systems managers must send a proposed notice at least 120 days before implementing a new, amended or altered system to the DA Freedom of Information and Privacy Office. The proposed or altered notice must include a narrative statement and supporting documentation. A narrative statement must contain the following items:

(i) System identifier and name;

(ii) Responsible Official, title, and phone number;

(iii) If a new system, the purpose of establishing the system or if an altered system, nature of changes proposed;

(iv) Authority for maintenance of the system;

(v) Probable or potential effects of the system on the privacy of individuals;

(vi) Whether the system is being maintained, in whole or in part, by a contractor;

(vii) Steps taken to minimize risk of unauthorized access;

(viii) Routine use compatibility;

(ix) Office of Management and Budget information collection requirements; and

(x) Supporting documentation as an attachment. Also as an attachment should be the proposed new or altered